

Internet + diefstal (cyber crime)



Grootste probleem van nu is de BABEL TRUC

Pierre Janssen woonachtig in Roggel



- **Opleiding HBO en Universitair** en al meer als 40 jaar ervaring en in **beveiliging werkzaam**, Een Technische achtergrond: computertechnologie, Computernetwerken, Product manager **communications**,
- Werkzaam geweest in **Nederland, Brussel, Zweden, en Ierland**, Product Manager communications en controls, Manager Detectie app. en buiten beveiligingssystemen, Kluis detectie voor banken,
- **Docent voor de beveiligings opleidingen** in Nederland : MBV, Technisch beheerder TBV, IP doormelding, gecertificeerd docent aan UTC **universiteit Brussel**, Gast docent aan **Hoogeschool Utrecht**.
- **Geaccrediteerd docent** Opfris cursus/VRKI - TBV/MBV vanuit het CIBV een van de 5 opleiders in Nederland die de opleiding wettelijk mag geven. En lid van toezicht bij de opleiders
- **Schrijver van:** HBO Opleiding, Beveiliging, IP Netwerken en alarmering, MBO Opleiding Basis security, Hoofdstukken lesboeken MBV/TBV Kenteq, IP-alarmering ,VEB handreiking IP doormelding, Maas Opleidingen, Hoogeschool Utrecht deel boeken geschreven, Hoofdstukken lesboek bij Van Dusseldorp opleidingen
- **Nu eigen bedrijf** Security Technologie voor ontwikkelen van lesstof en Consultancy voor installateurs voor project begeleiding. Het verzorgen van cursussen en Schrijven van Opleidingen voor de Beveiliging industrie op maat bij bedrijven.



Security technologie

Consultancy

Technical writer

Digitale Weerbaarheid

Kleding kopen, je bankzaken regelen of een aanvraag bij de gemeente, je regelt het allemaal gemakkelijk online. Het internet maakt ons dagelijks leven aangenamer. Tegelijkertijd blijkt uit de Online Veiligheidsmonitor dat slechts één op de drie Nederlanders zich echt veilig voelt online en geeft slechts een kwart aan dat ze over voldoende kennis beschikken om hun online veiligheid te waarborgen.



Presentatie:

Babbeltruc,s en de gevaren die voor ieder op de loer liggen

1. Een van de onderwerpen van cybercrime is wel de babbeltruc
2. Hoe groot is het probleem nu ?
3. Gevaren en vormen van oplichting vaak ook via internet waarbij criminelen zich voordoen als medewerkers van helpdesk of bankpersoneel, bel fraude, belasting of incasso bedrijven etc.
4. Direct aangifte doen en politie waarschuwen
5. Waar kan ik hulp zoeken





Wat is de Babbeltruc

Babbeltrucs zijn smoesjes waarmee criminelen mensen proberen op te lichten.

De oplichters ogen vaak betrouwbaar. Ze bellen op, komen aan de deur of spreken mensen aan op straat met een mooie smoes.

Vervolgens stelen zij geld en andere waardevolle bezittingen. In sommige gevallen gebeurt dit in combinatie met bedreiging en/of geweld.

De oplichters doen zich soms ook voor als meteropnemer, reparateur of politieagent. Of ze zeggen bijvoorbeeld dat ze van de bank zijn of van de thuiszorg.

Ook vragen ze soms om een glas water of een pen, terwijl een handlanger het huis binnenglipt



Aantal incidenten met nepagenten blijft stijgen,

Het aantal incidenten waarbij ouderen worden opgelicht door criminelen die zich voordoen als agent blijft stijgen.

De teller staat voor het **eerste halfjaar van 2025 al op 6496 incidenten**. In heel 2024 werden 8329 incidenten met nepagenten geregistreerd.

Elke dag registreert de politie zo'n 35 meldingen van deze slinkse babbeltrucs. Criminelen bellen of schrijven eerst, vaak met het dreigende nieuws over inbraken in de buurt. Daarna staan ze aan de deur, zogenaamd als agent, om sieraden, contant geld en zelfs bankpassen met pincode 'veilig te stellen'.

Gevaren en vormen van oplichting **ook via het internet** waarbij criminelen zich voordoen als medewerkers van helpdesk of bankpersoneel, bel fraude, belasting of incasso bedrijven etc.



Vraag? halen mannen of vrouwen vaker babbeltrucs uit?

Dat kun je eigenlijk niet zeggen. Zowel mannen als vrouwen doen het. Het voordeel van vrouwen is dat ouderen bevattelijker zijn om daar hulp aan te bieden. Wat dat betreft kan je eigenlijk geen onderscheid maken.'

Wat zijn goede tips om een babbeldief je huis uit te krijgen?

Ik wil dat u nu mijn huis verlaat en als u dat niet doet, bel ik de politie." Zo simpel is het.

Desnoods, als je het niet vertrouwt of niet durft, bel je even de buurvrouw of familie. **Als je vraagt of diegene langs wil komen, is dat voor de babbeldief vaak al genoeg om weg te gaan.**

Die babbeldief wil immers graag anoniem blijven.'



Zijn het altijd oudere mensen die in babbeltrucs trappen?

'Nee, zeker niet', Maar vaak wel, hoewel ook jongeren erin trappen.

Veel mensen schamen zich, dat zoiets hen is overkomen.

'Daardoor doen ze niet makkelijk aangifte.

Het zijn vooral ouderen van wie kinderen hebben gezegd 'Pap, mam, niet zomaar opendoen. Om dan tóch tegen je kinderen te zeggen dat het je is overkomen...

Ze zijn bang dat ze dan op hun donder krijgen, dus houden ze hun mond maar.'

Dat mensen toch opendoen, ondanks de waarschuwingen, heeft verschillende redenen,

'Sommige mensen denken dat het ze niet overkomt of vinden het zielig. Soms is het een stukje angst of naïviteit



Schaam je niet, het kan iedereen overkomen

Iedereen kan slachtoffer worden van online oplichting, of Babbeltruc's. Ik heb IT'ers gehad die slachtoffer werden van **WhatsApp-fraude** en bankmedewerkers die slachtoffer zijn geworden van beleggingsfraude."

Wat zijn voorbeelden van een babbeltruc? En hoe begint

'Iemand belt bij je aan en vraagt: 'Ik heb ontzettend veel dorst, mag ik misschien een glaasje water?', 'Ik heb net een ongeluk gehad, wilt u de garage of politie bellen?', 'Ik sta met een lege benzinetank, mag ik misschien tien euro lenen?' of: 'Mijn kind moet plassen, mag hij bij u naar het toilet?'

Een babbeltruc is vaak een hulpvraag,





Werkwijze bij Babbeltrucs

Babbeltrucs zijn smoesjes waarmee criminelen proberen mensen op te lichten. Deze criminelen misleiden u door te doen alsof ze bijvoorbeeld een medewerker van de thuiszorg, bank of politie (zogenoemde nepagent) zijn.

De nepagenten bellen u vaak eerst op of ze sturen een brief. Ze verwijzen dan naar (gewapende) inbraken in uw buurt en geven aan dat u daar ook het slachtoffer van lijkt te worden. Ze bieden aan om uw waardevolle eigendommen daarom snel bij u thuis op te halen en zogenaamd veilig te bewaren.

Soms geven ze daarbij een code door, die de persoon aan de deur aan u zal doorgeven. Dit doen de oplichters om vertrouwen te wekken.

Daarna komen er inderdaad mensen aan de deur die zich voordoen als iemand van de politie. Ze gebruiken daarbij vaak namen van agenten.

Het komt voor dat zij zich dan legitimeren met een vals pasje. Soms hebben ze (een deel) van een (nep)uniform aan en noemen ze de code die eerder is doorgegeven.



Wat kunt u doen tegen nepagenten?

Als u bent gebeld:

- Hang direct op als u wordt gebeld door iemand die zegt van de politie te zijn en die vraagt naar kostbaarheden zoals sieraden of bankgegevens.
- Bel de politie via 0900-8844 en controleer via hen of u echt gebeld bent door een politiemedewerker.
- Als u informatie heeft doorgegeven: laat niemand binnen.





Als er iemand aan de deur staat:

- Doe de deur niet zomaar open voor iemand die zegt van de politie te zijn. Vraag eerst om het politielegitimatie en personeelsnummer van degene die voor de deur staat en bel ook in dit geval de politie via 112 om het nummer te checken.
- Een echte politieagent kan zich altijd legitimeren met een geldig politielegitimatiebewijs. Dat is een kaart met daarop de naam, het personeelsnummer en een pasfoto. Dit bewijs is een kaart gemaakt van polycarbonaat, net zoals het rijbewijs. Ook heeft het politielegitimatiebewijs meerdere zichtbare en onzichtbare echtheidskenmerken zodat deze minder eenvoudig is te vervalsen. [Bekijk hier een voorbeeld.](#)

Een politiemedewerker in 'burgerkleding' **moet altijd** uit eigen beweging het politielegitimatiebewijs laten zien.



Achterkant van een politielegitimatiebewijs





Ik ben gebeld door mijn bank

Oplichters doen zich voor als medewerkers van U bank en bellen met de mededeling dat Uw bankrekening in gevaar is. Doordat zij gebruikmaken van de techniek "spoofing" ziet U het nummer van uw bank, terwijl de oplichters in werkelijkheid met een ander nummer bellen. Zo proberen zij Uw vertrouwen te winnen, zodat U geld overmaakt of inlog-gegevens afgeeft

Dit kunt U direct doen

Hang op en bel zelf uw bank op met het U bekende nummer. En vraag na of uw bank u inderdaad gebeld heeft.

ING en de Rabo app voor telebankieren hebben een toets voor direct contact met de bank om te controleren of U gebeld word door een bankmedewerker op dat moment

Druk op  p'  en dan in 2^e menu **op "bel"**

INSTALLEER NOOIT SOFTWARE DIE DE BESTURING VAN JE COMPUTER OVERNEEMT

- Je bank vraagt nooit om software te installeren (zoals Anydesk Teamviewer en LogMein) waarmee zij op afstand jouw computer, tablet of smartphone kunnen bedienen.

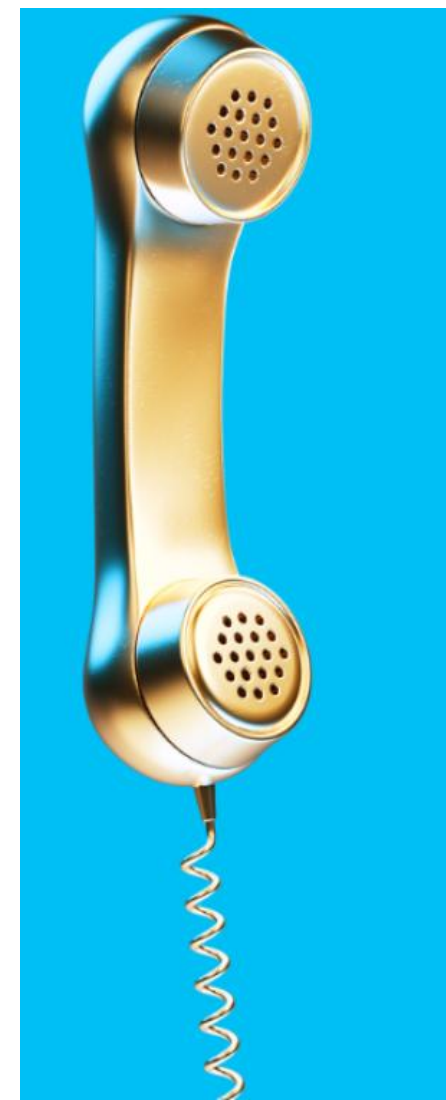
Deze signalen wijzen op fraude

U moet Uw geld overboeken naar een zogenaamde “veilige rekening” omdat er spraken zou zijn van een digitale dreiging of fraude, **Of een veilige kluis opslag !!!! Kluis ?**

De oplichters vragen U om in te loggen in Uw bankomgeving of Uw inloggegevens en/of pincode door te geven

Het gebeurt ook dat oplichters iemand naar U toesturen om uw bankpasje en/of waardevolle spullen op te halen en “veilig te stellen”

- Heb je een nieuwe betaalpas ontvangen? Onthoud: knip de chip. Na het doorknippen van de betaalchip (het goudkleurige vierkantje op de pas) kun je je oude pas weggooien bij het restafval. Als je alleen de kaart, maar niet de chip doormidden knipt, kan een oplichter met de doorgeknipte betaalpas (en je pincode) nog steeds geld opnemen bij een geldautomaat.





Babbeltrucs en veilig pinnen

- Pin indien mogelijk binnen bij een bank, maar wees ook daar alert en pin veilig.

Laat u niet afleiden. Ook niet als iemand zegt dat u bijvoorbeeld een bankbiljet of iets anders liet vallen.

Denkt u dat het geld toch van u is? Stop dit dan in uw jaszak en niet in uw portemonnee.

- Staat iemand te dicht bij u? Vraag voordat u gaat pinnen of deze persoon een stukje naar achteren gaat. Bent u met zijn tweeën? Laat dan de tweede persoon zorgen dat er afstand blijft.





is voor veilig pinnen

- Houd **je pincode strikt geheim** en exclusief voor je betaalpas.
- Berg je pas goed op in een afgesloten gedeelte in je jas of tas.
- Ziet je vaste pinautomaat er anders uit? Gebruik hem niet.
- Dek met je hand je pincode af en laat je niet afleiden. Meelezers maken zo geen kans.
- Houd je afschrijvingen in de gaten.
- Stel indien mogelijk een opname- en kredietlimiet in. Hoe meer je kunt rood staan, des te groter de kans op meer schade.
- Meld onterechte afschrijvingen zo snel mogelijk bij de bank.
- Bedenk dat je bank je nooit zal vragen je betaalpas op te sturen. Ook niet om deze af te geven aan iemand die bij je langskomt.
- Bankpas kwijt of gestolen? Blokkeer hem meteen.





Security technologie

Consultancy

Technical writer

Een barcode voor de digitale wereld.

Een QR-code is altijd gelinkt aan een bepaalde website of een app. Wie ergens een QR-code ziet, kan deze vierkante zwart-witte barcode met de camera van de smartphone scannen. Via een tik op een verschenen link, opent dan direct de bijbehorende site.





Security technologie

Consultancy

Technical writer

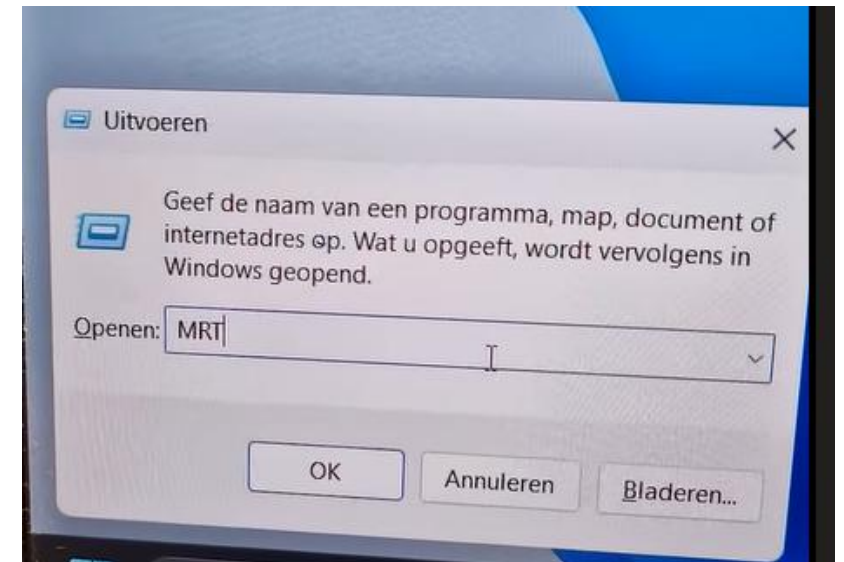
Hoe controleert U of schadelijke software op Uw PC staat

Window 11 heeft een extra functie in combinatie met de window toets



Window plus toets “R” opent nieuw venster

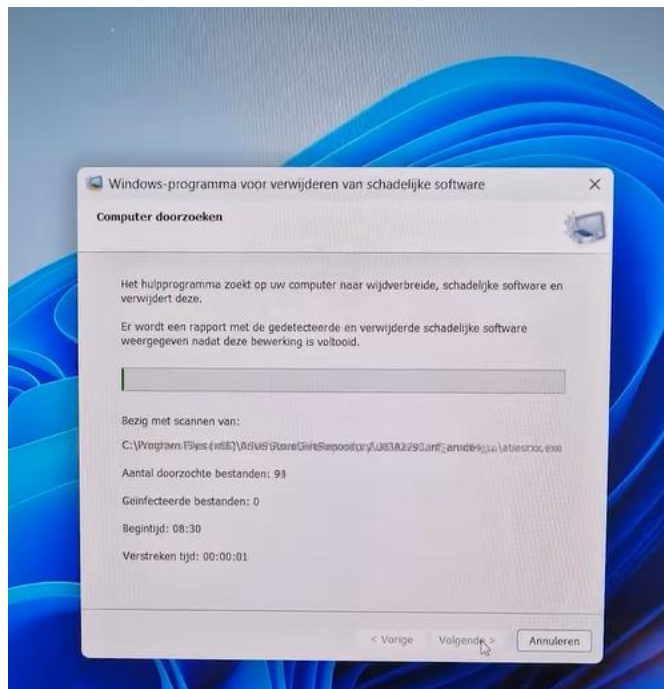
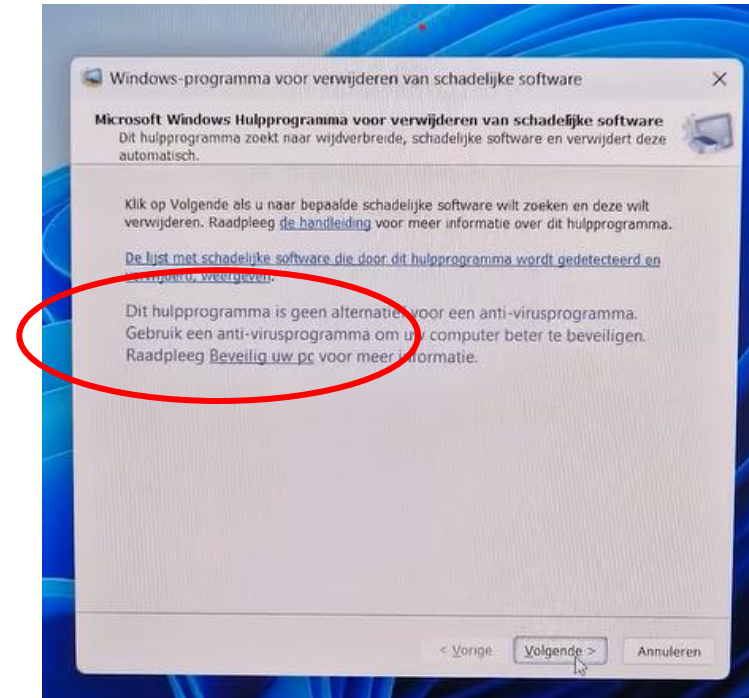
En kijk of en MRT in de balk staat en druk OK



Vervolg op controle

Het volgend scherm opent in Windows en
klik op “volgende”

In volgende scherm selecteert u de scantype

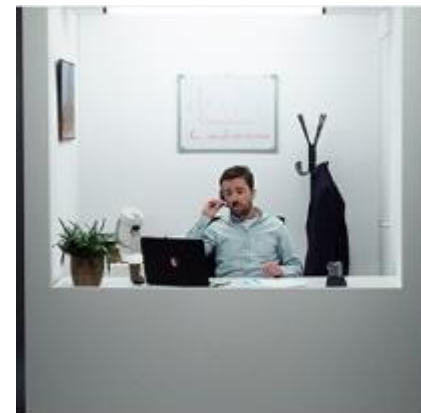


Windows start nu met zoeken naar
schadelijke software en zal hiervan
een melding geven en verwijderen

Groene balk geeft proces weer:



Ik had contact met een helpdesk ivm computer problemen



Oplichters doen zich voor als medewerkers van de helpdesk van een groot bedrijf. Om u goed te kunnen helpen vragen ze u software te downloaden waarmee ze op afstand problemen met uw computer kunnen oplossen. In werkelijkheid krijgen ze zo toegang tot uw bankomgeving en/of gevoelige informatie.

Dit kunt u direct doen

- Hang direct op wanneer u ongevraagd benaderd wordt door een helpdesk en ga niet in op pop-ups die waarschuwen dat contact met een helpdesk nodig is.
- Download nooit software op verzoek van een onbekende (helpdesk).
- Zoekt u zelf contact met een helpdesk, controleer dan de contactgegevens: oplichters maken namelijk ook gebruik van valse websites waarop ze zich voordoen als de helpdesk van bekende bedrijven.

Gebeld door een Incasso bureau of de belastingen

Oplichters doen zich voor als een incassobureau of de Belastingdienst en bellen u over een openstaande factuur of belastingachterstand.

Om beslaglegging te voorkomen, moet de openstaande factuur direct worden betaald. Sommige oplichters vragen meer geld dan het zogenaamd openstaande bedrag. U zou bijvoorbeeld een betalingsachterstand hebben van 300 euro, maar er wordt geadviseerd 3000 euro te betalen. Wat u teveel betaalt wordt later weer teruggestort. In werkelijkheid bent u het geld kwijt.

Advies

Gaat het om een incassobureau, vraag dan eerst om de openstaande factuur en om een bewijs van de overeenkomst. Verbreek vervolgens de verbinding. Krijgt u niets toegestuurd, dan weet u zeker dat het om een niet bestaand incassobureau gaat. Krijgt u wel iets toegestuurd, controleer dan of het om een bestaand en betrouwbaar incassobureau gaat. Dit kan b.v. in [het register van de Kamer van Koophandel](#).

Gaat het om de Belastingdienst, verbreek dan de verbinding en bel zelf terug. Gebruik daarvoor de telefoonnummers uit uw eigen administratie of die op de website van de Belastingdienst en controleer of er daadwerkelijk een achterstand betaald moet worden.



Security technologie

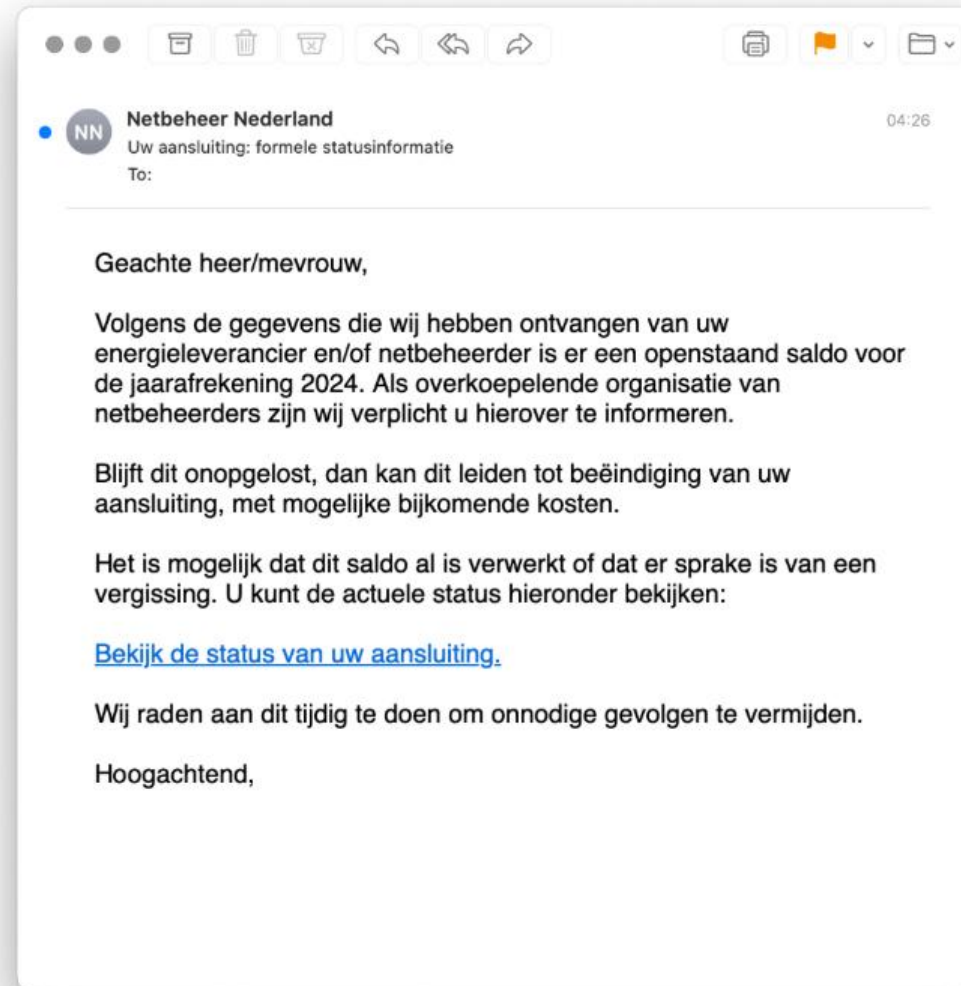
Consultancy

Technical writer

Mail van Net beheerder over openstaande factuur

Bij ons zijn meerdere meldingen binnengekomen over phishingberichten. Onze naam wordt hier misbruikt door kwaadwillenden. In de mails geven ze aan dat er een betaalachterstand bij je energieleverancier of netbeheerder is. Verwijder het bericht direct en klik niet op links.

Deze mail gaat rond
vanaf 28-08-2025



Hulp na een babbeltruc

Een babbeltruc is altijd een vorm van misleiding.

Onbekenden spreken je aan, Ze gebruiken smoezen om je vertrouwen te winnen.

Vervolgens stelen zij je geld, bankpas en pincode of waardevolle bezittingen. Op de volgende pagina's lees je wat je kunt doen na babbeltrucs.

Dit kun je doen na een babbeltruc

- Doe altijd aangifte bij de politie of bank. Lees hoe je jouw [aangifte kan voorbereiden](#)
- Is je pinpas of creditcard gestolen? Of stelen dieven geld van je rekening? Blokkeer je pasjes via de Bankpassen Meldcentrale. Bel [0800 - 0313](#) of vanuit het buitenland [+31 \(0\)88 - 38 55 372](#). Je kunt ook contact opnemen met je bank.



Security technologie

Consultancy

Technical writer

Hoe vind ik de juiste Hulp voor mij ?

En waar



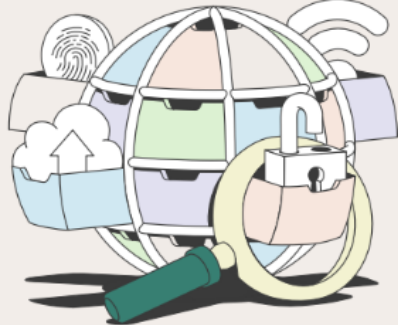
veiliginternetten.nl



alertonline.nl

 veiliginternetten.nl

 Menu



Veilig internetten begint hier

Waar ben je naar op zoek? Wat is cryptojacking?

AangifteAccountdiefstalAIAAlert onlineAppsBack-upmeer +

Nieuws Nieuws

Cybercrime meldingen in juni #1

6 juni 2025

Nieuws Nieuws

Politie Noord-Nederland nu digitaal ter plaatse

6 juni 2025

Nieuws Nieuws

Politie haalt wereldwijd illegale netwerken offline om cybercriminaliteit te bestrijden

23 mei 2025

Nieuws Nieuws

Thuiswerkvacatures: nieuwe vorm van vacaturefraude

20 mei 2025

Nieuws Nieuws

Jongeren steeds vaker online geronseld voor criminele activiteiten

15 mei 2025

Nieuws Nieuws

Wat is een AI-hiring scam?

14 mei 2025

Nieuws Nieuws

Themamaand Online Seksueel Geweld

13 mei 2025

Nieuws Nieuws

EchtNietVandaag regio Rotterdam

13 mei 2025

Nieuws Nieuws

Oplichting met de aanvraag van je visum of ETA

30 april 2025

Nieuws Nieuws

Cyberbeeld april

30 april 2025

Nieuws Nieuws

Als je niet wilt dat Meta AI traint met jouw data, kan je bezwaar maken

Nieuws Nieuws

TikTok introduceert dashboard voor extra beveiliging

24 april 2025

Dagelijks gebruik Nieuws

Veilig internetten begint hier

Aangifte x

Mijn WhatsApp is gehackt



Accountdiefstal

AI

Alert online

Basisbeveiliging

Cybercrime

Cyberpesten

Dagelijks gebruik

Datalek

Digitaal opgroeien

Digitale veiligheid

Fraude

Gamen

Geldzaken

Hulpvraagfraude

Intimidatie

Mobiel

Phishing

Privacy

Reputatieschade

Senioren en online veiligheid

Social media

Veilig op reis

Aangifte

Gebeurt er iets vervelends op internet, zoals oplichting, afpersing, sextortion of word je online gepest? Of is er sprake van diefstal van je gegevens? Dan kun je aangifte doen bij de politie. Of melden bij www.helpwanted.nl of www.fraudehelpdesk.nl

Aangifte

Vraag

Wat moet ik doen als er een naar filmpje/nare foto van mijn kind online staat?

Aangifte

Vraag

Waar kan ik aangifte van doen of een melding van maken bij een cybercrime?

Aangifte

Nieuws

19-jarige voor vierde keer aangehouden voor phishing
17 september 2024

Intimidatie

Vraag

Wat moet ik doen als er een naar filmpje/nare foto van mij online staat?

Aangifte

Nieuws

Alléén jij bepaalt wat er van jou online staat
17 oktober 2024

Cybercrime

Nieuws

Politie Midden-Nederland komt thuis langs bij digitale criminaliteit
17 april 2024

Intimidatie

Vraag

Wat moet ik doen als ik word afgeperst met naaktbeelden?

Aangifte

Vraag

Ben ik slachtoffer van identiteitsfraude, en wat kan ik doen?

Aangifte

Vraag

Hoe vind ik de juiste helpdesk?

Social media

Vraag

Waar kan mijn kind hulp vinden na een vervelende online

Privacy

Vraag

Wat is doxing?

Aangifte

Nieuws

Politie rolt netwerk op dat persoonsgegevens stal
5 november 2024

Aangifte

Vraag

Wat kan ik doen als ik online word gepest?

Zijn er nog vragen ?

